

PASSWORD MANAGER > AUTOFILL

Disable a Browser's Built-in Password Manager

View in the help center:
<https://bitwarden.com/help/disable-browser-autofill/>

Disable a Browser's Built-in Password Manager

If you are new to Bitwarden, it's likely that the web browser you use has been saving and autofilling your passwords. Most web browsers enable this by default, but experts generally agree that [built-in password managers are more vulnerable](#) than dedicated solutions like Bitwarden.

For that reason, and because an active built-in password manager can interfere with your Bitwarden experience, we recommend disabling your web browser's built-in password manager.

Note

The Bitwarden browser extension can be deployed across managed endpoints. Learn more about [deploying the Bitwarden browser extension to managed devices](#).

Learn how to disable the built-in password manager for major browsers:

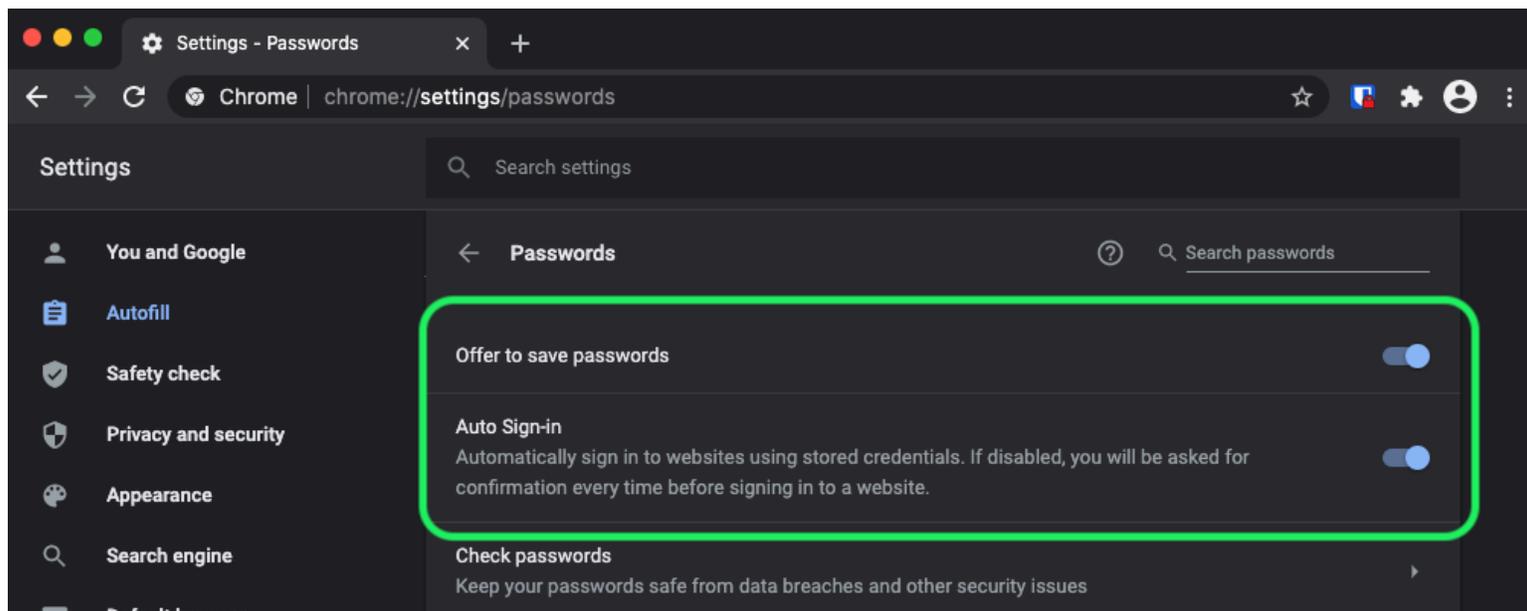
Tip

Several modern browsers, including Edge, Opera, and Brave, use a Google Chrome framework called "Chromium". If you are using one of those browsers, use the **Chrome/Chromium** instructions.

⇒Chrome/Chromium

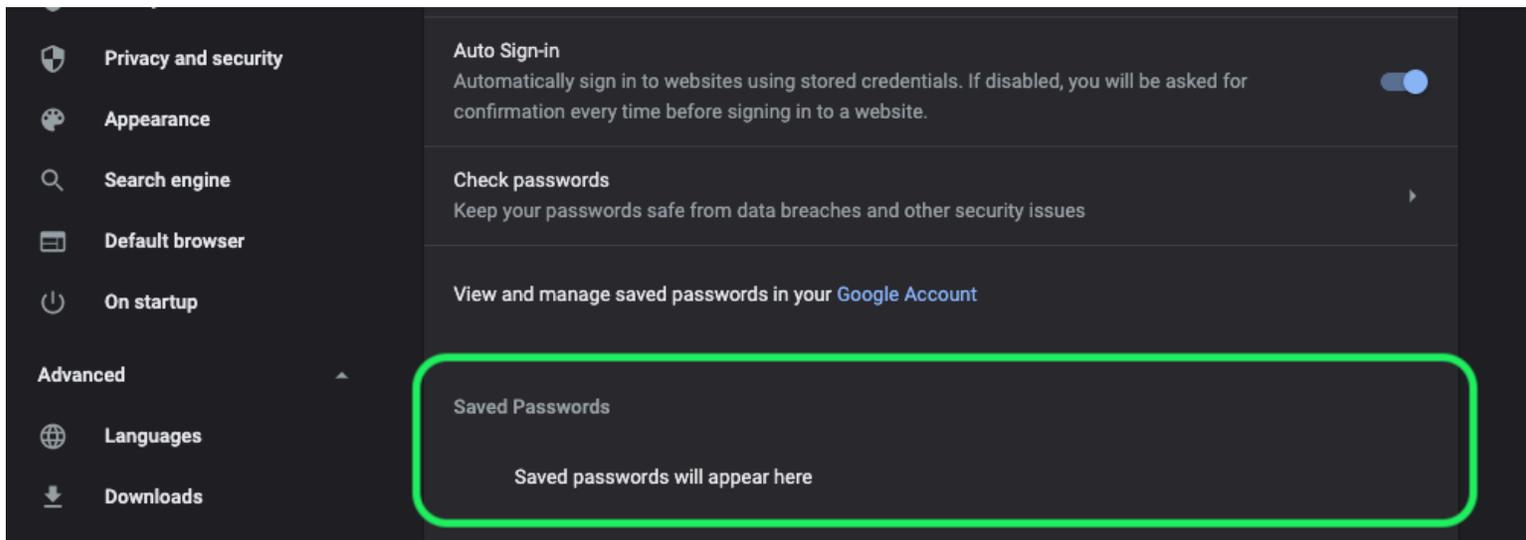
In Chrome or any Chromium-based browser (Edge, Opera, and Brave), navigate to the **Passwords** page by entering `chrome://password-manager/settings` in the address bar, substituting `chrome` for your browser name (for example, `brave://password-manager/settings`). For Edge users, navigate to `edge://wallet/settings`.

On this page, toggle off both the **Offer to save passwords** option and the **Auto Sign-in** option:



Chrome Password Options

This page will also list any **Saved Passwords** that are being stored by the browser:

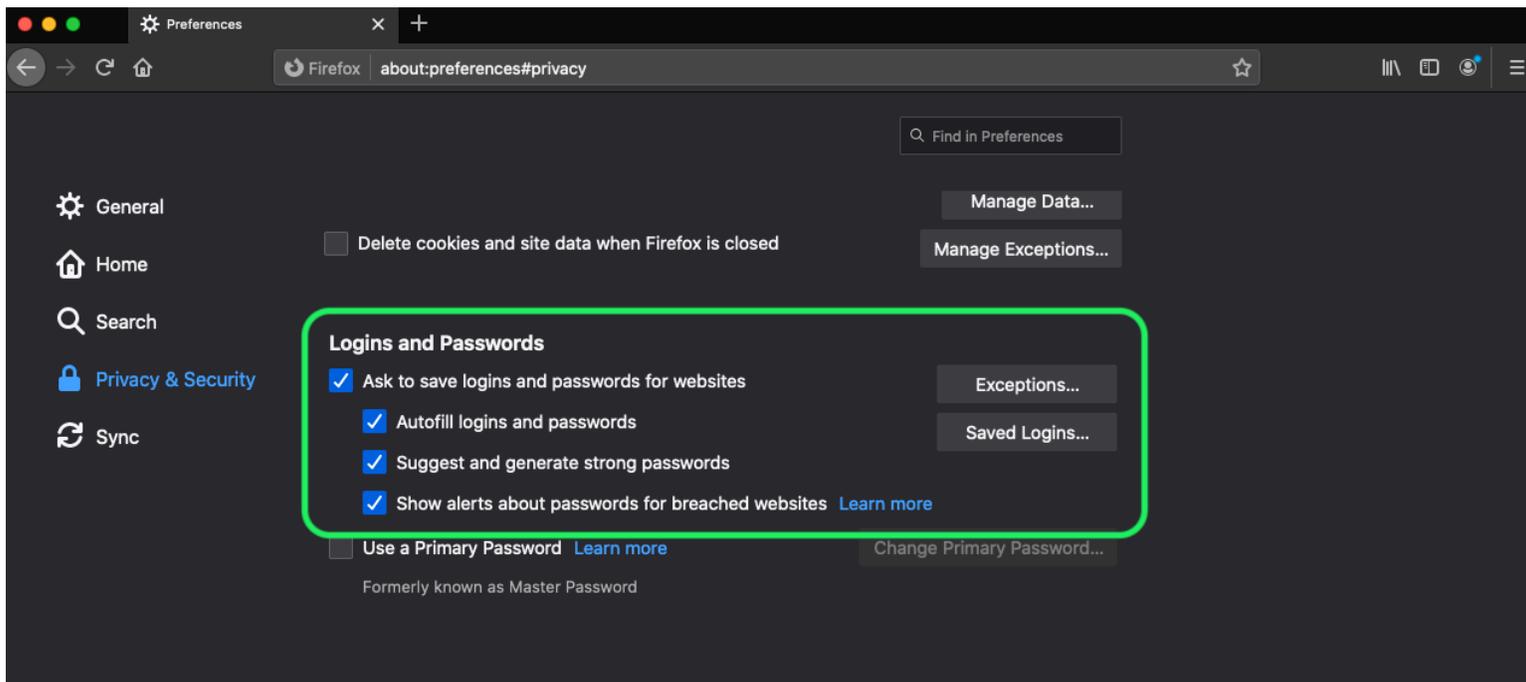


Chrome Saved Passwords

If you haven't already saved these passwords in Bitwarden, [export them](#) to prepare for future import to Bitwarden. Once exported, you should delete these passwords from the browser's storage.

⇒Firefox

In Firefox, navigate to **Preferences** → **Privacy & Security** and scroll down to the **Logins and Passwords** section. In this section, uncheck all the pre-checked options:

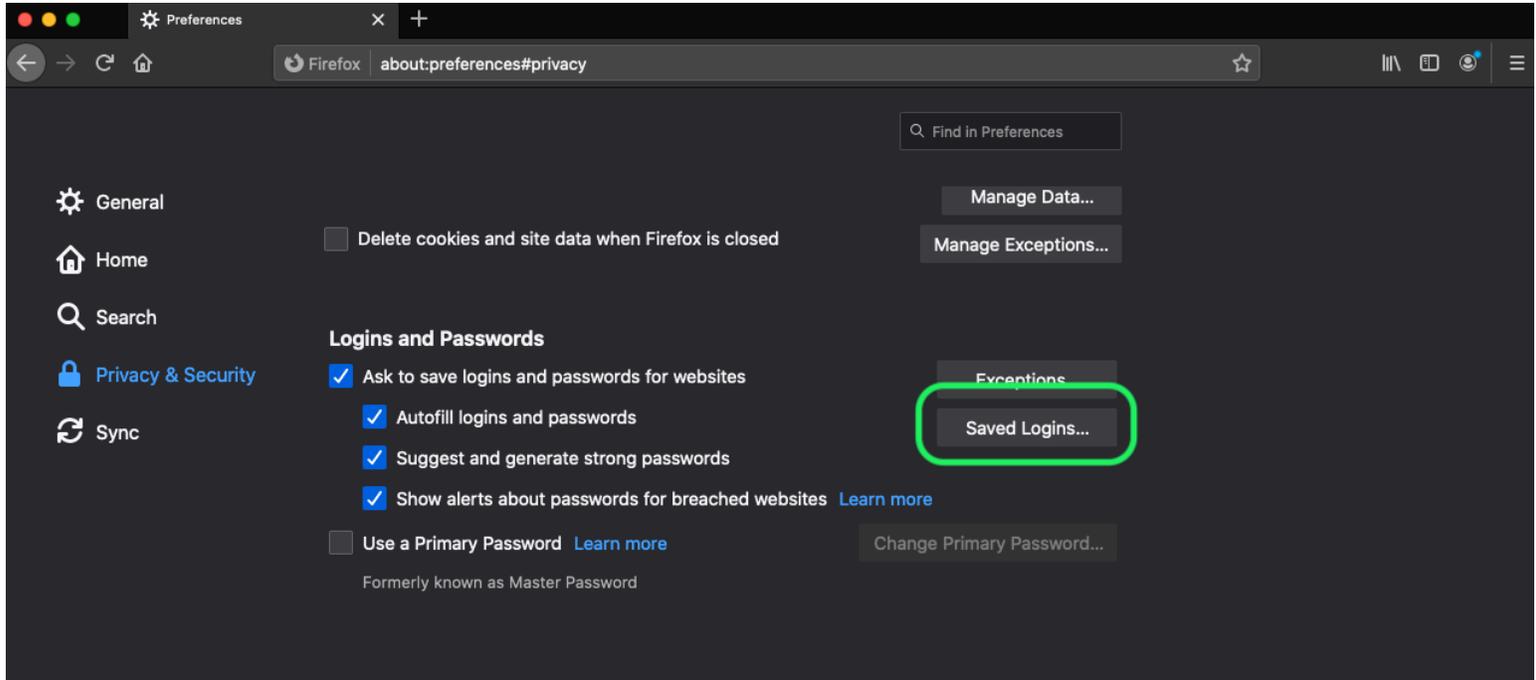


Firefox Password Options

💡 Tip

Bitwarden Password Manager offers a variety of [reports](#) for premium users, like the Exposed Passwords and Reused Passwords reports, and a **free Data Breach report for all users**.

You should also find out which logins Firefox has already saved by selecting the **Saved Logins...** button:

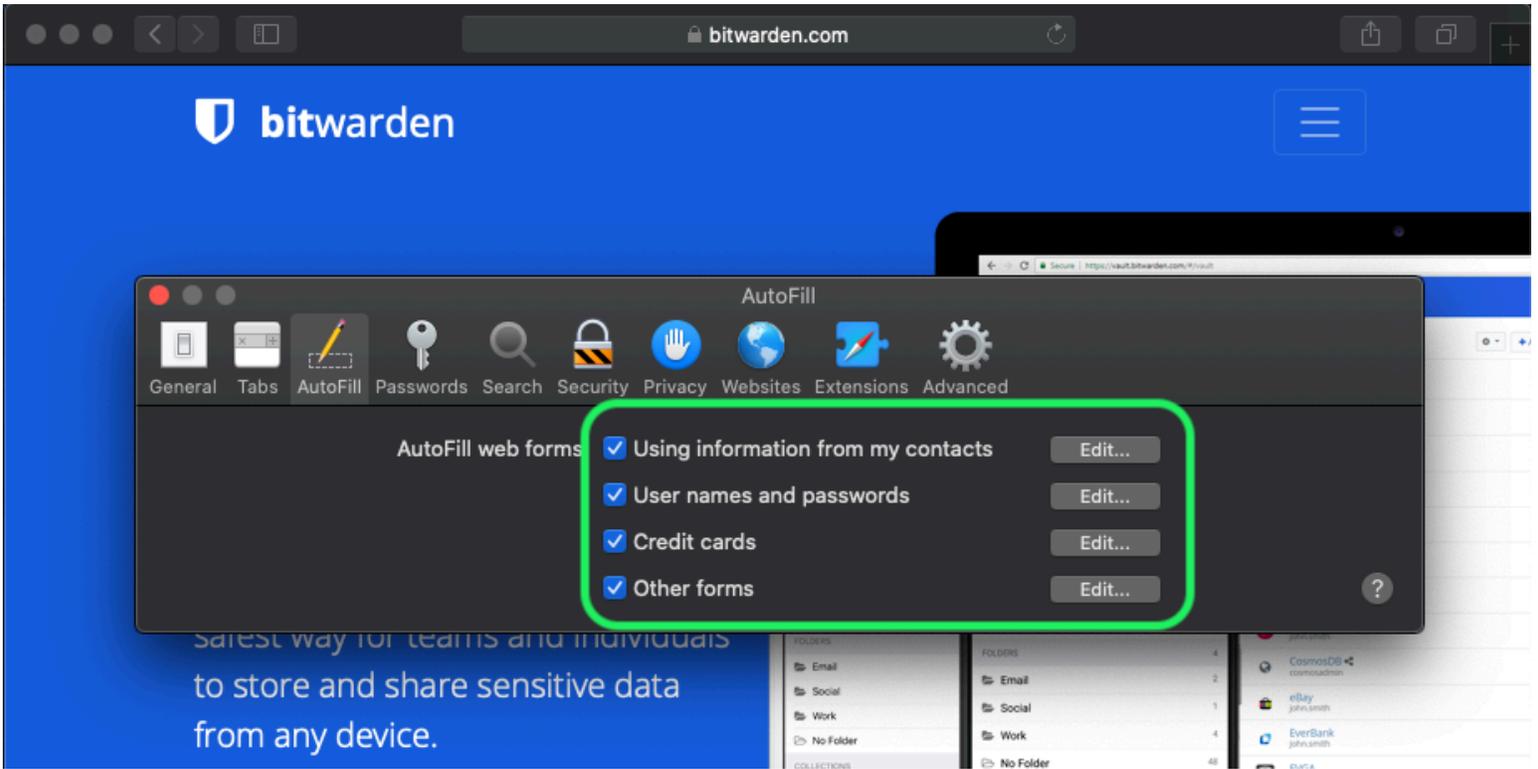


Firefox Saved Logins

If you haven't already saved these passwords in Bitwarden, [export them](#) for future import to Bitwarden. Once exported, you should  **Remove** these passwords from Firefox.

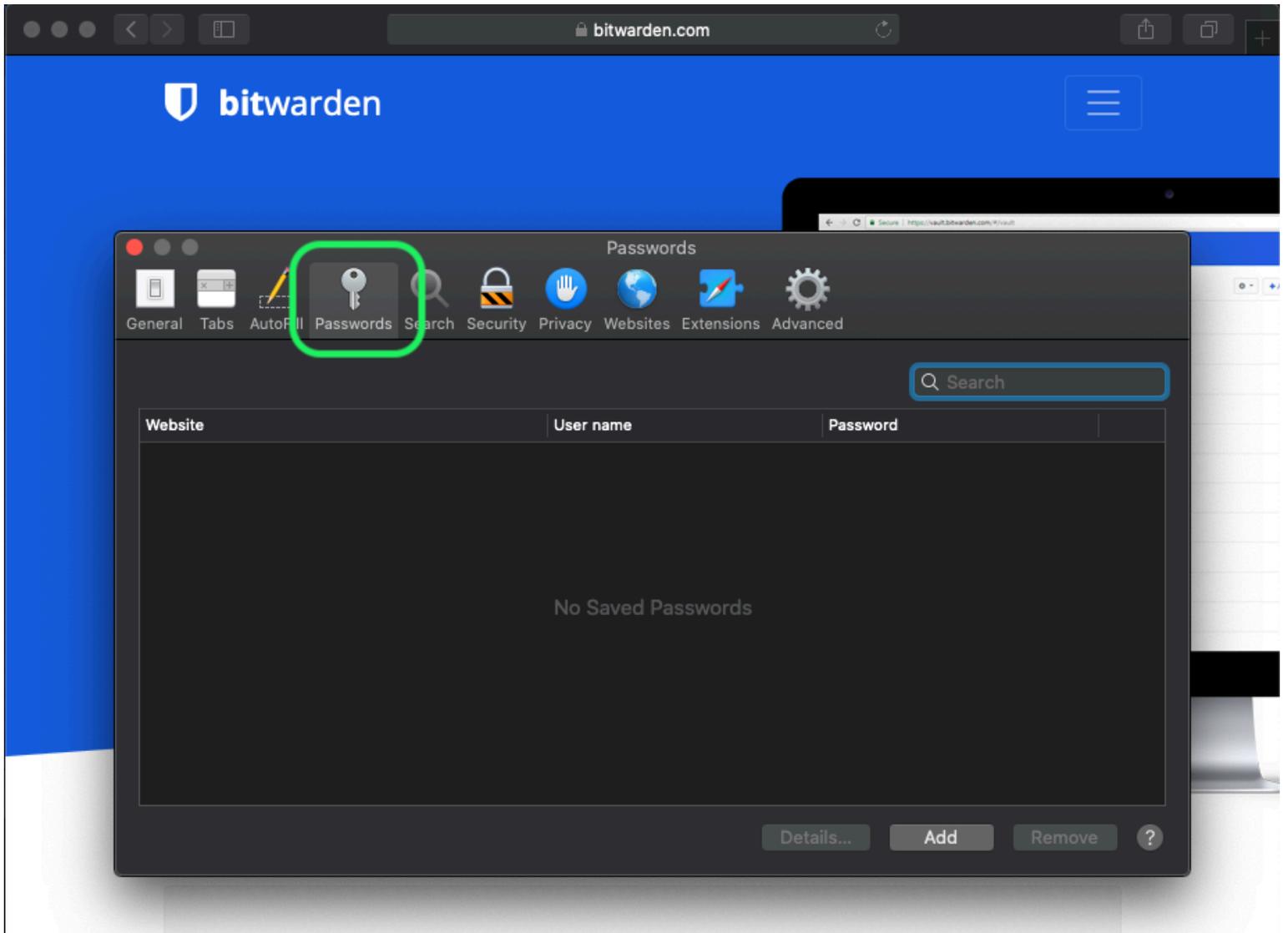
⇒Safari

In Safari, open **Preferences** from the menu bar and navigate to the **AutoFill** tab. On this tab, uncheck all the pre-checked options:



Safari Password Options

You should also find out which passwords Safari has already saved by navigating to the **Passwords** tab:

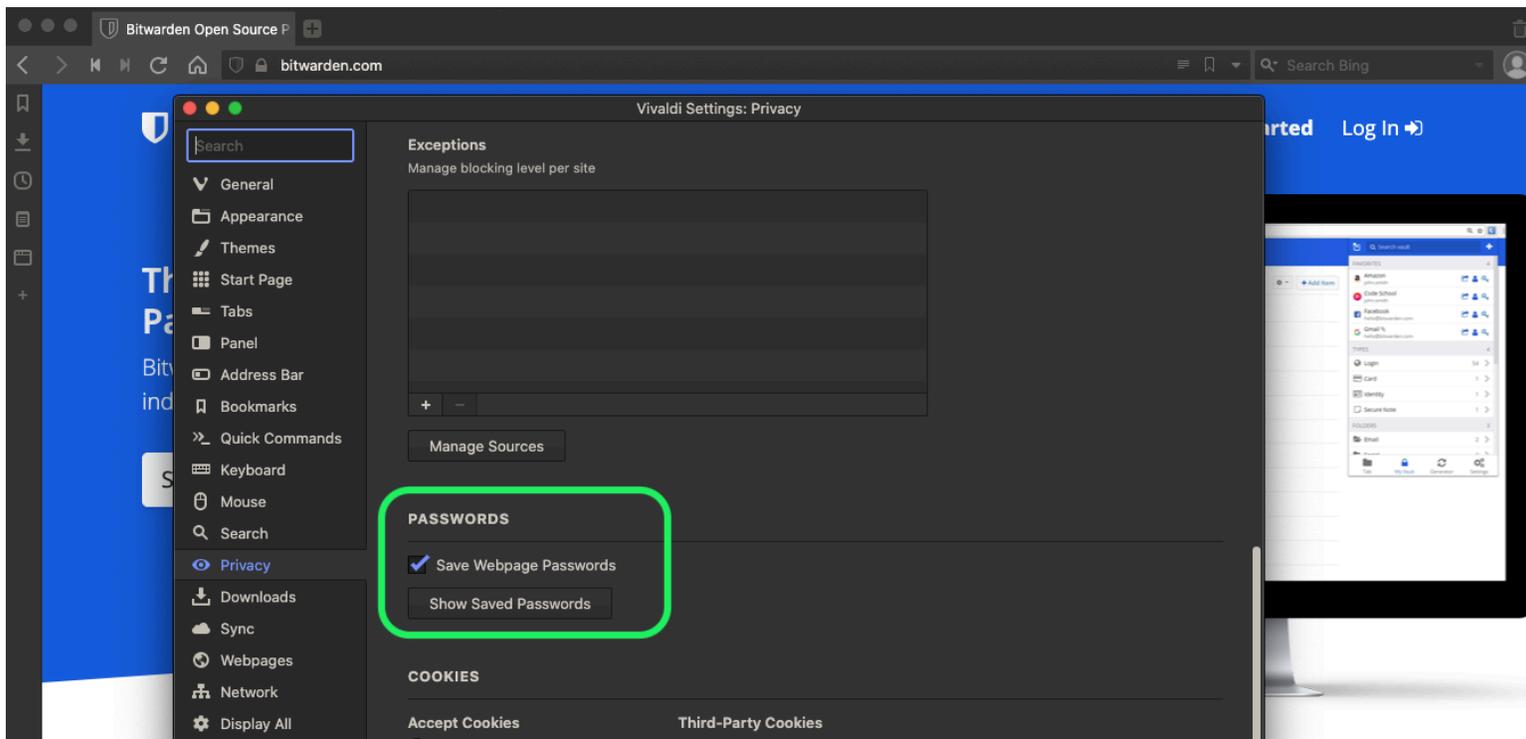


Safari Saved Passwords

If you haven't already saved these passwords in Bitwarden, create login items in Bitwarden for these passwords. Once all saved passwords are in Bitwarden, **Remove** these passwords from Safari.

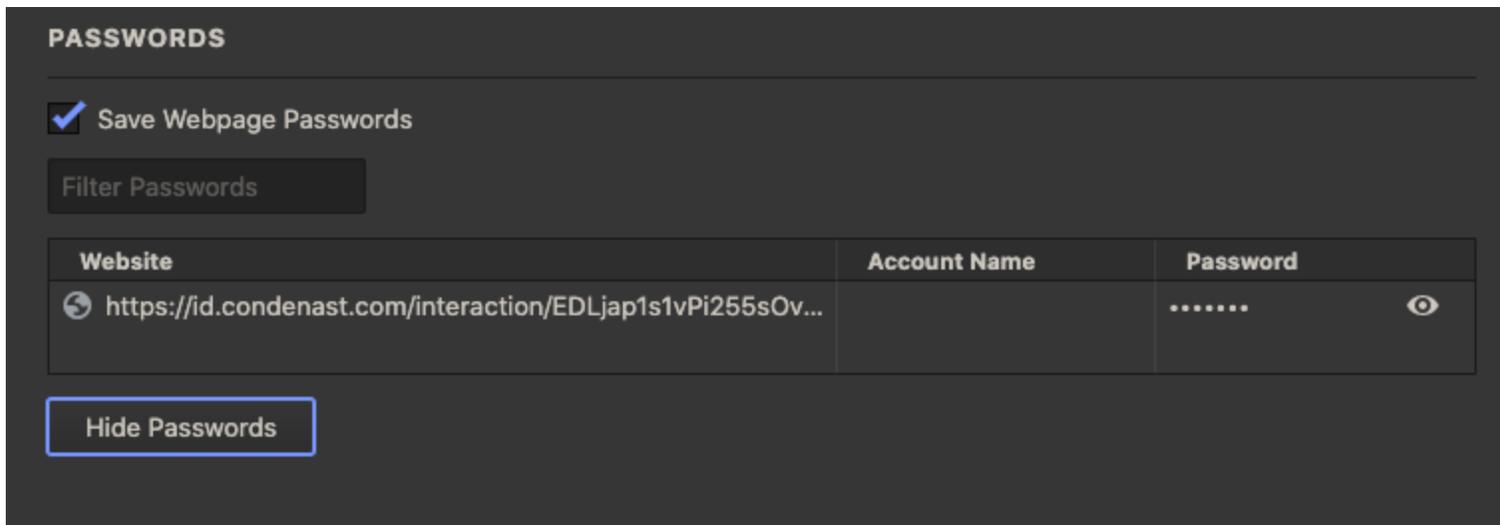
⇒Vivaldi

In Vivaldi, open the **Vivaldi Settings** window and select **Privacy** from the left-hand navigation. Scroll down to the Passwords section and uncheck the **Save Webpage Passwords** option:



Vivaldi Password Options

You should also find out which passwords Vivaldi has already saved by selecting the **Show Saved Passwords** button:



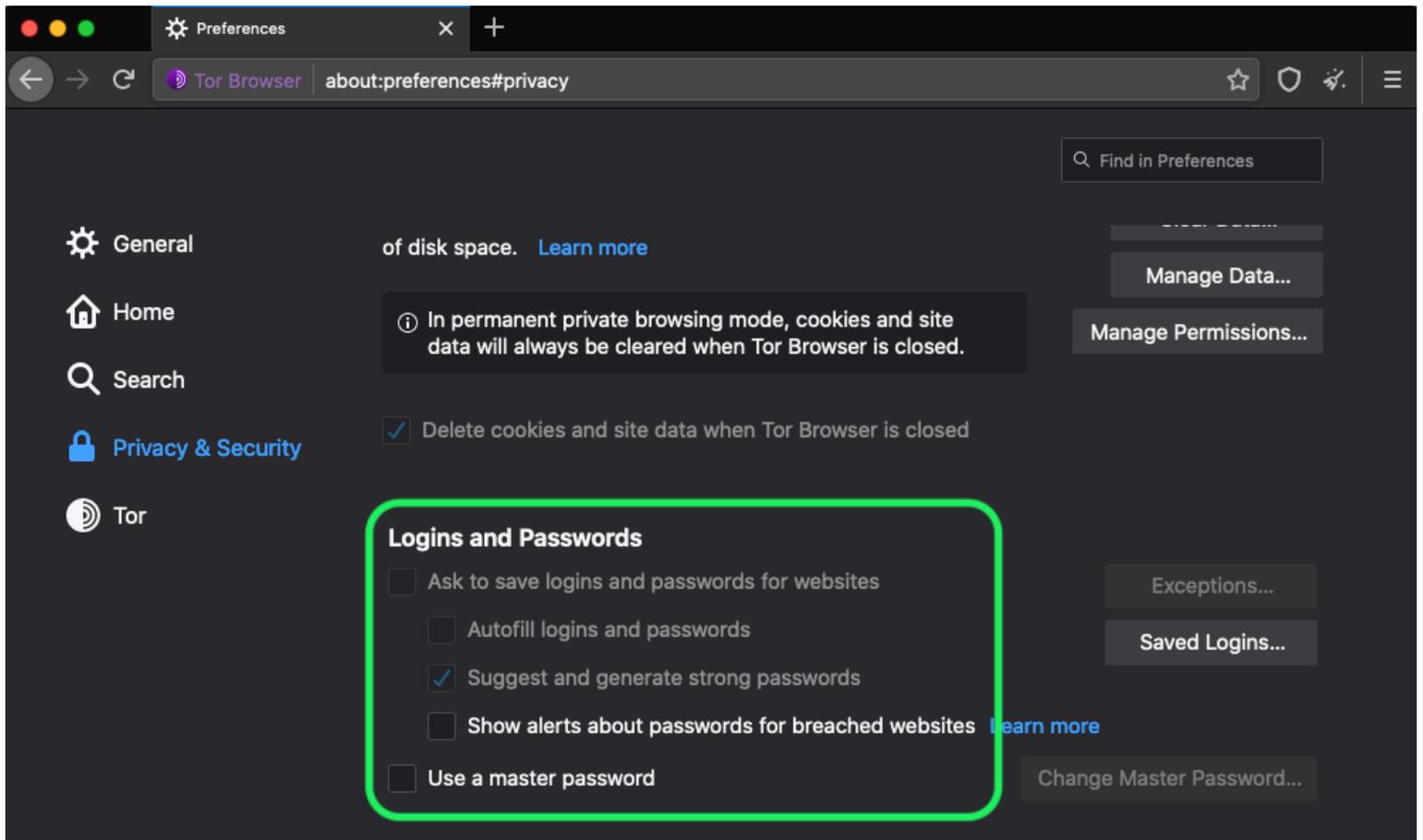
Vivaldi Saved Passwords

If you haven't already saved these passwords in Bitwarden, create login items in Bitwarden for these passwords. Once all saved passwords are in Bitwarden, remove these passwords from Vivaldi. [Learn how.](#)

⇒Tor

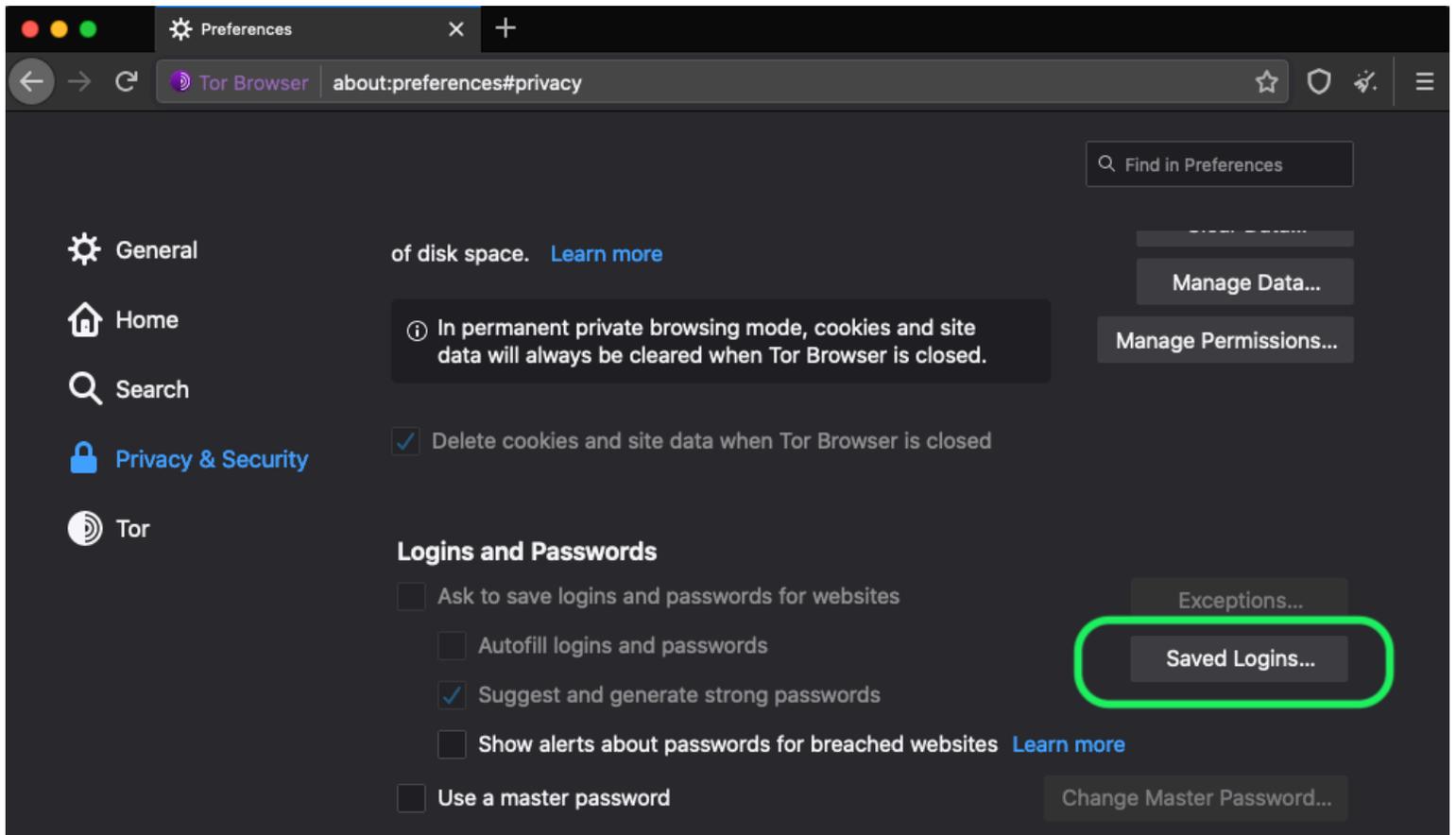
Despite sharing roots with Firefox, Tor is unique in that it doesn't save your logins by default. If you haven't manually configured Tor to save and autofill logins, you are already all set.

If you did, navigate to the **Passwords** page by entering `about:preferences#privacy` in the address bar, and scroll down to the Logins and Passwords section. Toggle off all the options that you had checked:



Tor Password Option

You should also find out which logins Tor has already saved by selecting the **Saved Logins...** button:

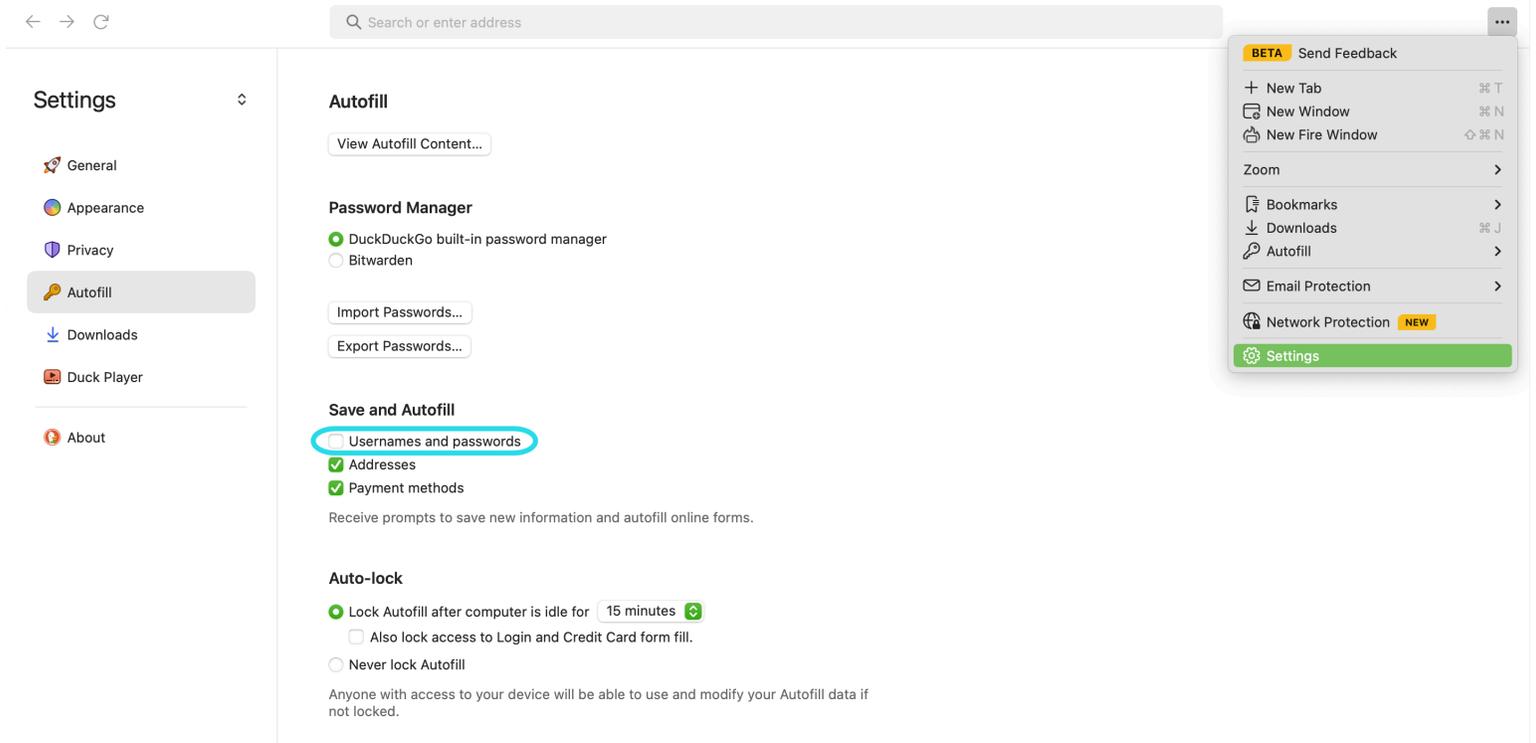


Tor Saved Passwords

If you haven't already saved these passwords in Bitwarden, create login items in Bitwarden for these passwords. Once all saved passwords are in Bitwarden, **Remove** these passwords from Tor.

⇒ DuckDuckGo

In DuckDuckGo, navigate to **Settings** → **Autofill**. From this screen, uncheck the box for **Username and passwords**.



Disable DuckDuckGo Password Manager

You can create a backup of your existing data by selecting **Export Passwords**. Once you have created a backup file, select **View Autofill Content...** and delete the stored autofill data to remove previously saved suggestions.

In the Password Manager section, macOS users can choose to use Bitwarden. Learn more about the Bitwarden DuckDuckGo macOS browser integration [here](#).